Information Disclosure Vulnerability, as well as Information Disclosure, Tampering, and Denial-of-Service (DoS) Vulnerability in "EcoGuideTAB"

Release date: July 10, 2025
Mitsubishi Electric Corporation

Overview

Information disclosure vulnerability due to Weak Password Requirements (CWE-521[1]), as well as information disclosure, tampering, and denial-of-service (DoS) vulnerability due to Use of Hard-coded Credentials (CWE-798[2]), exist in photovoltaic system monitor "EcoGuideTAB" (discontinued in 2015, support ended in 2020). An attacker within the Wi-Fi communication range (approximately 10 meters) between the units of the product (measurement unit and display unit) may be able to derive the password from the SSID (CVE-2025-5022). Furthermore, by exploiting this vulnerability (CVE-2025-5022), an attacker who has access the Wi-Fi communication between the units may use hardcoded user ID and password common to the product series to disclose information such as generated power and electricity sold back to the grid stored in the product, tamper with or destroy stored or configured information in the product, or cause a Denial-of-Service (DoS) condition on the product (CVE-2025-5023).

However, the product is not affected by these vulnerabilities when it remains unused for a certain period of time (default: 5 minutes) and enters the power-saving mode with the display unit's LCD screen turned off.

The names of the products affected by these vulnerabilities are listed below. Please discontinue the use of the affected products or take mitigation measures.

Note that devices related to power generation, such as PV modules, PV junction boxes, and PV inverters connected to the product, are not affected by these vulnerabilities. Furthermore, the product does not store any personal or sensitive information.

CVSS[3]

CVE-2025-5022	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score: 6.5
CVE-2025-5023	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H	Base Score: 7.1

Affected products

All versions of the models listed below are affected.

PV-DR004J
PV-DR004JA

Description

Multiple vulnerabilities below exist in Photovoltaic System Monitor "EcoGuideTAB".

- CVE-2025-5022: Information disclosure vulnerability due to Weak Password Requirements (CWE-521)
- CVE-2025-5023: Information disclosure, tampering, and denial-of-service (DoS) vulnerability due to Use of Hard-coded Credentials (CWE-798)

Impact

An attacker within the Wi-Fi communication range between the units of the product (measurement unit and display unit) may be able to derive the password from the SSID. Furthermore, by exploiting this vulnerability, an attacker who has access the Wi-Fi communication between the units may use hardcoded user ID and password common to the product series to disclose information such as generated power and electricity sold back to the grid stored in the product, tamper with or destroy stored or configured information in the product, or cause a Denial-of-Service (DoS) condition on the product.

Note that devices related to power generation, such as PV modules, PV junction boxes, and PV inverters connected to the product, are not affected by these vulnerabilities. Furthermore, the product does not store any personal or sensitive information.

Countermeasures

As support for the affected products has ended, please discontinue their use or take mitigation measures.

Mitigations

For customers who are unable to immediately discontinue use of the product, Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities.

- Prevent an unauthorized third party that could be a malicious attacker from accessing the product's Wi-Fi communication range.
- Turn off the power of the display unit when not viewing data on the product.

---

1 https://cwe.mitre.org/data/definitions/521.html
2 https://cwe.mitre.org/data/definitions/798.html
3 https://www.first.org/cvss/v3.1/specification-document

Acknowledgement

Mitsubishi Electric would like to thank Rei Yano who reported these vulnerabilities.

Contact information

Contact us at the email address below if you have any inquiries regarding these vulnerabilities.

E-mail: taiyo@nm.MitsubishiElectric.co.jp